TESTBED IMPLEMENTATION OF LOOP-FREE SOFT HANDOFF IN WIRELESS BATTLEFIELD NETWORKS[1]

**Ibrahim Hökelek[*1], Selcuk Cevher[1,2], Mariusz A. Fecko[1], Provin Gurung[1], Sunil Samtani[1],
Zhensheng Zhang[3], Aristides Staikos[4], Jeffrey Bowcock[4]**

[1]Applied Research, Telcordia Technologies, Inc.
Piscataway, NJ 08854
{mfecko,ihokelek,pgurung,ssamtani}@research.telcordia.com

[2]City College of the City University of New York,
New York, NY 10031
cevhers@research.telcordia.com

[3]Argon ST,
San Diego, CA 92121
Zhensheng.Zhang@argonst.com

[4]U.S. Army CERDEC,
Fort Monmouth, NJ 07703
{Aristides.Staikos,Jeffrey.Bowcock}@us.army.mil

ABSTRACT

A fundamental challenge in wireless mobile battlefield networks (WMBNs) is frequent occurrence of wireless link congestion and failures due to blockage, mobility, interference, etc. In case of a link or node failure, the end-to-end session will be disrupted until the underlying routing protocol converges to its new path. We propose an innovative distributed architecture for a seamless multi-layer soft handoff protocol in WMBNs to provide the sub-second convergence in case of link/node failures[1]*. Our architecture utilizes a proactive "make-before-break" approach by introducing the concept of pre-computed remote Loop-Free Alternate Paths (LFAPs) on top of local LFAPs proposed by the IETF IP Fast-Reroute framework.*

We implemented this framework in the laboratory test bed using real COTS routers and collected statistics related to the convergence times and alternate path coverage ratios of local and remote LFAPs. The convergence experiments show that the convergence time of the remote LFAP mechanism is only slightly higher (a few 10s of milliseconds) compared to that of the local LFAP. Our coverage analysis showed that, by using only a small neighborhood (e.g., 2-hop neighborhood), a complete LFAP coverage can be achieved for most topologies generated by the BRITE topology generator. These results are significant since the IP fast reroute with a complete coverage can be achieved for WMBNs by introducing only a minimal overhead bounded within a small neighborhood.

1. INTRODUCTION

The characteristics of a wireless mobile battlefield network (WMBN) necessitate distinctive protocols specifically designed to meet WMBN requirements. A fundamental challenge in WMBN is frequent occurrence of wireless link congestion and failures due to blockage, mobility, interference, etc. In case of a link or node failure, the end-to-end session will be disrupted until the underlying routing protocol converges to its new path. The convergence time takes relatively long for link state routing protocols (LSRPs). This relatively long convergence time for LSRPs is not only intolerable by real-time applications but also significantly drops the throughput performance of WMBNs since limited bandwidth resources will not be efficiently used until a new route is converged.

The throughput degradation will be more severe if micro-loops are formed. A micro-loop is defined here as routing loop due to inconsistencies in the routers' FIBs (e.g., due to failure propagation and FIB update delays). In fact, the convergence time can be reduced to a sub-second value by setting configurable LSRP timers appropriately; however, smaller LSRP timers will not only significantly increase the signaling overhead in bandwidth limited WMBNs but also decrease the stability of LSRPs during frequent topology changes.

Currently IETF is standardizing IP Fast-ReRoute (IPFRR) mechanisms for both unicast and multicast type of traffic. IETF IPFRR draft [1] describes the fast-reroute framework, where the pre-computed repair paths are invoked immediately upon failure detection to minimize the adverse effects of link or node failures on the underlying routing protocols. In this framework, local Loop-Free Alternate Paths (LFAPs) [2] have been widely accepted as a viable solution. However, local LFAP can

[1] Prepared through the U.S. Army CERDEC programs: Seamless Soft Handoff Protocols, contract W15P7T-06-C-P820, and Proactive Integrated Link Selection for Network Robustness (PILSNER), contract W15P7T-04-C-P022.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE
01 DEC 2008

2. REPORT TYPE
N/A

3. DATES COVERED
-

4. TITLE AND SUBTITLE
Testbed Implementation Of Loop-Free Soft Handoff In Wireless Battlefield Networks

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Applied Research, Telcordia Technologies, Inc. Piscataway, NJ 08854

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM002187. Proceedings of the Army Science Conference (26th) Held in Orlando, Florida on 1-4 December 2008, The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**8**	

only partially cover the affected routes for only a single failure or failures within a shared risk link group. By using the concept of local LFAP as our starting point, we introduce remote LFAPs to achieve a complete fast reroute for multiple simultaneous failures with a minimal amount of extra complexity.

We propose an innovative distributed architecture for a seamless multi-layer soft handoff protocol in wireless battlefield networks to provide the sub-second convergence in case of link/node failures. In this architecture, a router that is adjacent to the failed resource immediately switches over pre-computed local LFAPs if LFAPs for protecting against this local failure exist (the same as IPFRR) and instantly propagates failure information to multi-hop neighbors (MNBs) (e.g., X-hop neighbors, where X is an integer number representing how many hops away failure information will be propagated). Upon receipt of failure information, MNBs activate their pre-computed LFAPs that they maintain for protecting against remote failures within their multi-hop neighborhoods.

We implemented this framework in the laboratory test bed using real COTS routers and collected statistics related to the convergence times and alternate path coverage ratios of local and remote LFAPs. Our coverage analysis showed that, by using only a small neighborhood (e.g., 2-hop neighborhood), a complete LFAP coverage can be achieved for most topologies generated by the BRITE topology generator. The convergence experiments show that the convergence time of the remote LFAP mechanism is slightly higher (a few 10s of milliseconds) compared to that of the local LFAP. These results are significant since the IP fast reroute with a complete coverage is achieved by introducing only the minimal overhead bounded within a small neighborhood.

2. SHA ARCHITECTURE

Our proposed Soft Handoff Agent (SHA) architecture has six key modules (see [4] for details), which are illustrated in Fig. 1. The *Monitoring* module collects real-time link state quality data such as Signal-to-Noise Ratio (SNR) via its interface to a radio management information base (MIB), and monitors the link state database of the WAN routers. The *Link Verifier* module sends a configurable small-sized heartbeat messages to verify the status of local links. The *Prediction* module implements proactive methods to predict the link quality in advance based on the information obtained via monitoring. The *Trigger* module which receives information from *Monitoring*, *Link Verifier*, and *Prediction* modules actually implements the decision logic to declare link/node failures and issues handoff triggers to the *Alternative Path Calculation (APC)* where actual switching to alternative path takes place. Finally, information relevant to failure detection is disseminated by *Controlled Dissemination* module.

A key module in this architecture is the *APC*, where local and remote LFAPs protecting the primary paths against anticipated failures are pre-computed and stored. We develop an innovative multi-hop neighborhood (MNBH) concept together with a remote LFAP algorithm to extend the IETF local LFAP approach. Our remote LFAP algorithm uses the well-defined IETF local LFAP equation iteratively within MNB and does not require extra information other than the neighborhood depth (i.e., the integer parameter X). In this framework, a router that is adjacent to the failed resource immediately switches over pre-computed local LFAPs if LFAPs for protecting against this local failure exist (the same as IETF IPFRR) and instantly propagates failure information to nodes within its MNBH. Upon receipt of failure information, nodes within MNBH activate their pre-computed remote LFAPs that they maintain for protecting against this remote failure. The main features of SHA are as follows:

- Complete prevention of micro-loops with a simple extension to IETF local LFAP mechanism
- Handling uncorrelated simultaneous failures
- Ability to distinguish link and node failures, and hence providing higher LFAP coverage
- Scalability by using innovative MNBH concept
- Minimal signaling overhead on top of IETF LFAP mechanism for fast failure notification

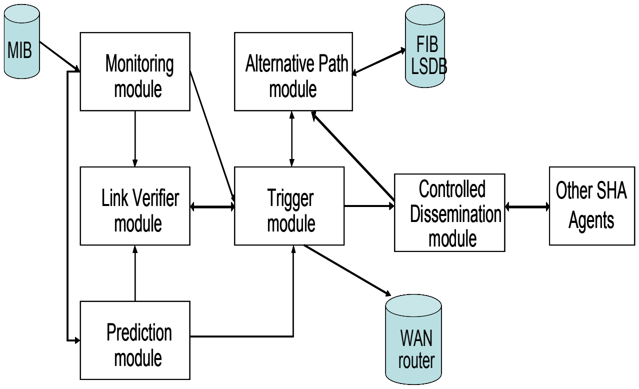

Fig. 1 Soft Handoff Control Agent Architecture components and interfaces with existing modules

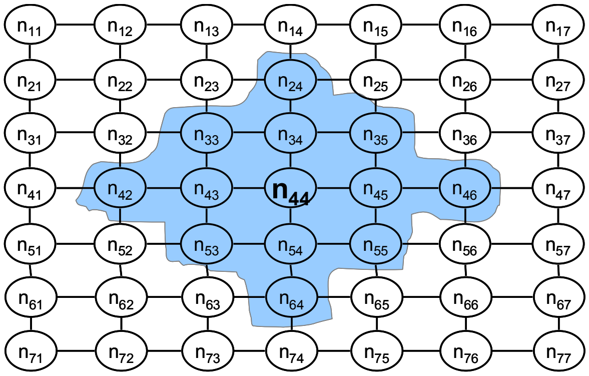

Fig. 2 Node n_{44}'s 2-hop neighborhood

3. DESIGN DETAILS

SHA achieves loop-free convergence by introducing two additional mechanisms on top of IETF IPFRR: multi-hop failure notification and remote LFAPs for protecting against failures at routers within multi-hop neighborhood. Apart from these two mechanisms, SHA implements all of its functionalities using the IETF IPFRR framework [1]. In this section, we first describe multi-hop neighborhood (MNBH) concept which is used to limit not only the scope of failure propagation for minimizing the extra overhead but also the number of the remote LFAPs for scalability. And then, an alternative path calculation algorithm for calculating local and remote LFAPs within MNBH is presented.

3.1. Multi-hop neighborhood

Fig. 2 shows an example network consists of 49 nodes. A node on the boundary has two neighbors if it is located on one of four corner positions (e.g., n_{11}); otherwise three neighbors (e.g., n_{12}). A non-boundary node has four neighbors (e.g., n_{22}). MNBH for each node only defines a local scope within which to propagate failure notifications. For example, 2-hop (i.e., X-hop where X=2) MNBH of *node* n_{11} consists of nodes (together with their adjacent links) which are at most 2-hop away from n_{11}. These nodes include n_{12}, n_{13}, n_{21}, n_{22}, and n_{31}; and hence, there are 5 nodes and 12 links within 2-hop MNBH of n_{11}. However, n_{44}'s 2-hop MNBH includes 12 nodes and 36 links as shown in Fig. 2. n_{44} has to calculate separate LFAPs for each destination in the network to protect against any combination of 12 node and 36 link failures. Since MNBHs are overlapping and define only a local scope for each node, no additional signaling mechanism is needed to explicitly maintain MNBHs in the network (e.g., a simple flooding mechanism similar to OSPF LSAs but limited to X-hop away routers is sufficient for maintaining MNBHs).

4. ALTERNATIVE PATH CALCULATION MODULE

In the literature, only local Loop Free Alternate Paths (LFAPs) with a well-defined equation for their calculations are used [2]. However, SHA uses both local and remote LFAPs; and hence a new LFAP calculation algorithm shown in Tale 1 is proposed. This algorithm is run at each node in a distributed manner to calculate both local and remote LFAPs based on the MNBH depth X.

This algorithm will be explained step by step using an example network shown in Fig. 3. We assume that node **n** is R1, the anticipated failure is for the link between routers R7 and R4, and the MNBH depth X is 1. A recursive X-hop neighborhood algorithm is used to find the X-hop (i.e., 1-hop) neighborhood (NBH) of R1. For example, R1's 1-hop NBH includes R1, R2, R7 and R8 and their interfaces (i.e., 1-hop NBH of R1). The link between R7-R4 is within R1's NBH due to R7's outgoing interface to R4. In this example, we only assume the anticipated failure of link R7-R4 but the same procedures will be repeated for other failures.

There are two distinct MNBHs used by the algorithm: one MNBH for R1 and another one for the link between R7 and R4, where the anticipated link failure is assumed. The first MNBH is used to decide what links should be protected by R1. However, the second MNBH defines the nodes which will receive the failure information when the link R7-R4 actually fails. For example link R7-R4 is directly connected to routers R7 and R4; and hence the failure information will be detected by both routers. R7's 1-hop NBH (i.e., X=1) includes R1, R2, R4 and R5 while R4's 1-hop NBH includes R4, R5, R7, and R9. Therefore, the failure information will be received by R1, R2, R4, R5, R7, and R9 (i.e., 1-hop NBH of link R7-R4).

In *Step 2b* of Tale 1, the algorithm finds all source-destination (s-d) pairs whose paths use the failed link R7-R4. Note that, in this step, source nodes are the ones only within 1-hop NBH of link R7-R4. The following s-d pairs are affected from the link R7-R4's failure: *R1-R3, R1-R4, R1-R9, R1-R6, R1-R5, R2 -R4, R4-R7, R4-R1, R4-R2, R4-R8, R5-R7, R5-R1, R5-R8, R7-R4, R7-R9, R7-R6, R7-R3, R9-R7, R9-R1,* and *R9-R8.*

Tale 1: Pseudo code for a loop-free alternative path calculation algorithm running at node n

```
Inputs: Network topology, node n, MNBH depth X
Outputs: A new routing table at node n for each
  anticipated link failure
1.  Find X-hop neighborhood ($X_n$) of node n
2.  For each anticipated failure of link i within $X_n$
        a. Find X-hop neighborhood ($X_i$) of
           failed link i
        b. Find all source-destination (s-d) pairs
           affected by link failure i, where source
           nodes are within $X_i$
        c. If there is an ECMP path which does
           not use link i, this path is an LFAP.
           Update safe LFAP existence matrix
           (SLEM)
        d. For all s-d pairs found in Step 2b
           excluding ones in Step 2c, apply both
           IETF local LFAP criteria and path
           safety check recursively until either all
           s-d pairs are repaired or no update is
           done for SLEM in last recursion
```

Note that from R1 to R3 there are two Equal Cost Multi Paths (ECMPS) and only one of them passes through the link R7-R4. We have to count ECMP paths as affected because both ECMP paths exist in the routing table of R1 and the one which uses the failed link will cause a micro-loop if it is not removed from the R1's routing table. However, the path which does not pass through the failed link R7-R4 can be used as an LFAP since it satisfies both local LFAP criteria and path safety check. As a result, there are 20 paths which are affected from the link R7-R4's failure. In *Step 2c* of Tale 1, R2 is used as loop-free alternative from R1 to R3 since the path from R2 to R3 does not pass through the failed link R7-R4.

In *Step 2d* of Tale 1, for all s-d pairs found in Step 2b whose primary paths use the failed link and do not have ECMPs, the algorithm applies IETF local LFAP criteria to check the existence of local LFAP. According to IETF local LFAP criteria in [2], a local LFAP exists at node y for a destination z when link between y *and* v fails if there is another neighbor (w, $w \neq v$) of y such that: $D(w,z) < D(w,y) + D(y,z)$. Here, the notation $D(w,z)$ is defined as the LSRP's shortest path distance from w to z. For the local LFAPs which satisfy the IETF criteria, we also introduce a new path safety condition since our algorithm considers remote failures. A local LFAP is safe if this LFAP does not pass through the failed link.

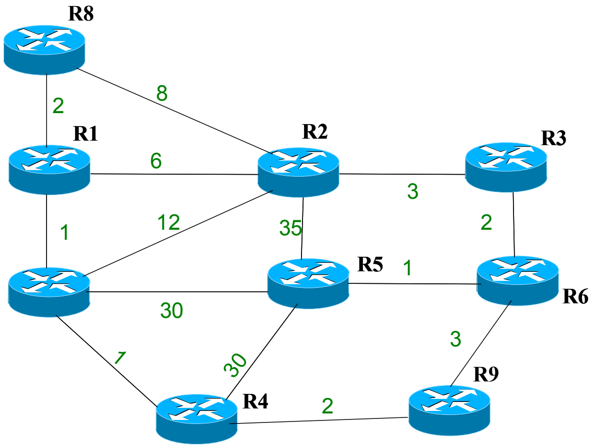

Fig. 3 Example Network Topology

After the first iteration in *Step 2d* of Tale 1, among 19 affected paths, 11 paths are repaired by local LFAPs. But there are 8 paths which do not have any local LFAP: *R1-R4, R4-R7, R4-R1, R4-R8, R7-R4, R9-R7, R9-R1,* and *R9-R8*. These s-d pairs need to be protected by remote LFAPs which will be calculated using a safe LFAP existence matrix (SLEM). So far, this matrix includes the primary paths which are not affected by the failure, ECMP paths, and local safe LFAPs found in the first iteration at *Step 2d* of Tale 1. By utilizing SLEM, if a node y's neighbor z has an LFAP to a certain destination v then node y can safely use z as its LFAP to v. SLEM is updated if a new s-d pair is repaired by LFAP. For example, R4 can reach to R7 via R5 (i.e., local LFAP) and SLEM entry for R4 to R7 is updated to reflect this fact. Using SLEM, R9 finds that it can safely reach R1 and R8 via R4 (i.e., remote LFAP). *Step 2d* of Tale 1 will repeat this procedure until either all s-d pairs are covered or there is no update for SLEM at the last iteration. After completing the second iteration at *Step 2d* of Tale 1, all s-d pairs are repaired: R1-R4 (via R2), R4-R7 (via R5), R4-R1 (via R5), R4-R8 (via R5), R6-R7 (via R5), R6-R1 (via R5), R7-R4 (via R2), and R9-R7 (via R4).

Table 2 and Table 3 show the routing tables for R1 before the link R7-R4 fails and after the alternative path calculation algorithm is modified according the neighborhood depth X is 1. Note that routing entries are updated for destinations *R3, R4, R9, R6, and R5.* For the destination R4, there is no local LFAP and hence our algorithm finds a remote LFAP via R2.

Table 2: R1's primary routing table before failure

To	*Next*	*Cost*
R2	R2	6
R3	R2 or R7	9
R4	R7	1
R5	R7	8
R6	R7	7
R7	R7	1
R8	R8	2
R9	R7	4

Table 3: R1's routing table after LFAPs are installed for link failure R7-R4

To	*Next*	*Cost*
R2	R2	6
R3	R2	9
R4	R2	16
R5	R2	12
R6	R2	11
R7	R7	1
R8	R8	2
R9	R2	14

5. TESTBED IMPLEMENTATION

Fig. 4 shows our testbed which consists of 7 emulated WIN-T nodes. Each node consists of a Cisco router representing the Wide Area Network (WAN) router, SHA technology running on general purpose processor (GPP), traffic source/sink, and radio as shown in Fig. 5. Cisco Internetwork Operating System (IOS) Release 12.3 is used on the WAN router. In this environment, we implemented multi-threaded SHA program in Java where there are six different threads: i) main SHA, ii) link verifier sender, iii) link verifier receiver, iv) failure notification sender, v) failure notification receiver, and vi) LFAP installer.

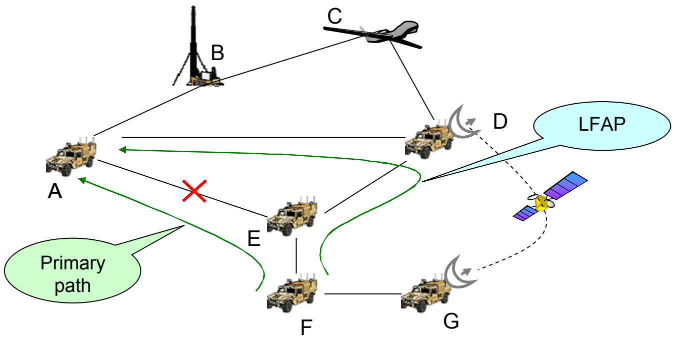

Fig. 4 The 7-node network topology for local LFAP convergence experiments

Main SHA periodically reads the network topology from the router's Link State Database (LSDB), runs the alternate path calculation algorithm to calculate local and remote LFAPs, and store them in temporary routing table objects to be immediately installed to the WAN router when actual link failures are detected. *Link verifier sender* periodically sends small size UDP request (REQ) messages to all of its immediate neighbors and waits for their reply (REP) messages. A neighbor's *link verifier receiver* immediately sends a REP message when it receives a new REQ. By using REQ and REP messages, several statistics such as round trip times and timeout value to declare the packet lost are dynamically maintained. *Main SHA* checks these statistics periodically in small intervals and declares a failure if the number of REP messages which are not received within a timeout value exceeds a certain threshold. Upon failure detection, *main SHA* creates two new threads: one for installing LFAPs and another for sending failure notification messages to X-hop nodes. *LFAP installer* installs LFAPs, which are pre-computed and stored in a temporary routing table object to protect against the corresponding failure, to the WAN router. *Failure notification sender* uses TCP communication to send the failure notification messages to X-hop nodes reliably.

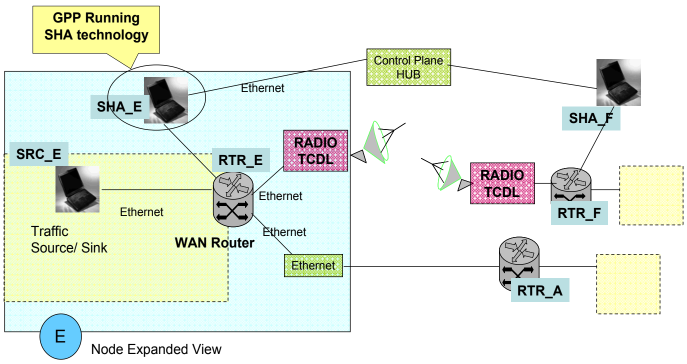

Fig. 5 Expanded view of a single node

6. CONVERGENCE EXPERIMENTS

We performed the convergence analysis of our new fast reroute mechanism using 7-node PILSNER testbed consisting of 2600 and 3600 series Cisco routers as shown in Fig. 4 and Fig. 6. OSPF link costs are set to the same value for all links. A dedicated computer (e.g., an SHA agent), which is running our fast reroute technology, is connected to each router through an Ethernet cable. These agents obtain the network topology from the routers in real-time by issuing an SNMP request. Using the retrieved network topology information, a set of LFAPs, which protects the failed primary paths when a real failure occurs, is pre-computed and stored. For both networks, the link between routers A and E is failed for all convergence experiments.

The convergence time on the alternate path is measured by running a session, similar to a ping application, between routers A and E. When the link between routers A and E is failed on the topology as shown in Fig. 4, the primary path A-E (and hence the session between them) fails. Once the failure is detected, the router A (E) reroutes its traffic over the alternate path A-D-E (E-D-A) by installing its pre-computed local LFAP. However, when the same scenario is applied to the topology in Fig. 6, there is no local LFAP in the router A (E) to protect the primary path A-E (E-A) for this failure. For the above scenario, our SHA technology propagates the failure information to router B (D) which is already pre-computed a set of remote LFAPs for this particular failure. As a result, the session is rerouted through the alternate path A-B-C-D-E (E-D-C-B-A).

For both local and remote LFAP scenarios, the experiments are repeated for 10 times and the mean convergence time is reported. The mean convergence time for the local LFAP scenario is measured 602 milliseconds while the mean convergence time for the remote LFAP scenario is 612 milliseconds. Note that LFAPs are stored in the agents which are external to the routers. These agents issue an IOS command to install the right set of LFAPs when a failure is detected. In reality, the agent technology should run in the router as a GPP and LFAPs should be installed beforehand and waiting for a failure signal to be activated. Therefore, a sub-100 ms convergence time should be possible if this technology is implemented within the router as a new protocol or extension to the existing link state routing protocols. A sub-second convergence time is adequate for the wireless mobile networks; however, for the backbone networks, the results should be used to compare the difference between local and remote LFAPs rather than their absolute values.

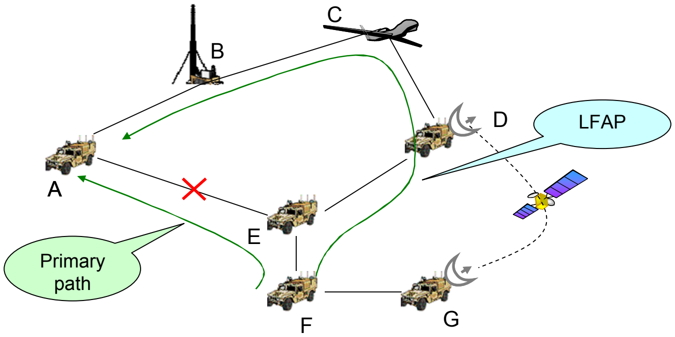

Fig. 6 The 7-node network topology for remote LFAP convergence experiments

The convergence times do not include the failure detection time since our primary objective in these experiments is to compare local and remote LFAP rather than proposing a new failure detection mechanism. For the sake of experiments, we implemented a heuristic based failure detection mechanism using periodic light-weight heartbeat messages similar to the Bidirectional Forwarding Detection. Note that the alternate path between A and E in the remote LFAP scenario is longer (A-D-E vs. A-B-C-D-E). The failure information is reached to one-hop neighbor within a few milliseconds since the round trip time between two neighboring agents is measured around 1-2 milliseconds. These results indicate that the convergence time of the remote LFAP mechanism is only slightly higher compared to the only local LFAP mechanism due to the failure notification time. This increase is bounded by the neighborhood depth times a few milliseconds.

However, the remote LFAP significantly increases the alternate path coverage since there is no local LFAP to protect the session between routers A and E when the link between routers A and E fails in Fig. 6. A more detailed coverage analysis is performed in the following section.

7. LFAP COVERAGE ANALYSIS

We performed the coverage analysis of our new fast reroute mechanism on realistic topologies generated by the BRITE topology generator in bottom-up mode [5]. The LFAP coverage percentage is defined here as the percentage of the number of LFAPs for protecting the primary paths which are failed because of link failures to the number of all failed primary paths. Only local LFAPs is considered in the coverage calculation for the neighborhood depth of 0 (i.e., X=0) while both local and remote LFAPs are taken into account when the neighborhood depth is set to a value greater than 0 (i.e., X>0).

The realistic topologies include AT&T and DFN using pre-determined BRITE parameter values from [5] and various random topologies with different number of nodes and varying network connectivity. For example, the number of nodes for AT&T and DFN are 154 and 30, respectively while the number of nodes for other random topologies is varied from 20 to 100. The BRITE parameters which are used in our topology generation process are summarized in Table 4 for random topologies (see [5] for the details of each parameter). In summary, *m* represents the average number of edges per node and is set to either 2 or 3. A uniform bandwidth distribution in the range 100-1024 Mbps is selected and the link cost is obtained deterministically from the link bandwidth (i.e., inversely proportional to the link bandwidth as used by many vendors). Since the values for *p(add)* and *beta* determine the number of edges in the generated topologies their values are varied to obtain network topologies with varying connectivity (e.g., sparse and dense).

The coverage percentage of our fast reroute method is reported for different network topologies (e.g., different number of nodes and varying network connectivity) using neighborhood depths of 0, 1, and 2. (i.e., X=0, 1, and 2). For a particular failure, LFAPs protecting the failed primary paths are calculated only by those nodes which are within the multi-hop neighborhood of this failure. Note that these nodes are determined by the parameter *X* as follows:

- For X=0,
  - Two nodes which are directly connected to the failed link
- For X=1,
  - Two nodes which are directly connected to the failed link and also neighboring nodes which are adjacent to one of the outgoing links of these two nodes
- And so on.

Table 4: BRITE topology generation parameters

	Bottom up
Grouping Model	Random pick
Model	GLP
Node Placement	Random
Growth Type	Incremental
Preferential Connectivity	On
BW Distribution	Uniform
Minimum BW	100
Maximum BW	1024
M	2-3
Number of Nodes	20,50,100
Number of ASs	50
p (add)	0.01, 0.05, 0.10
Beta	0.01, 0.05, 0.15

The LFAP coverage percentage for a certain topology is computed by the following formula:

$$\textbf{LFAP Coverage Percentage} = N_{lfaps}*100/N_{fpp}$$

where N_{lfaps} is the number of source-destination pairs whose primary paths are failed because of link failures and have LFAPs for protecting these failed paths. N_{fpp} is the number of source-destination pairs whose primary paths are failed because of link failures. The source-destination pairs, in which source and destination nodes do not have any physical connectivity after a failure, are excluded from N_{fpp} since none of the fast reroute mechanisms can protect these paths. Note that the coverage percentage includes a network-wide result which is calculated by averaging all coverage results obtained by individually failing all edges for a certain network topology.

Table 5 shows the LFAP coverage percentage results for random topologies with different number of nodes (*N*) and network connectivity.

Table 6 shows these results for AT&T and DFN topologies. In these tables, E_{mean} represents the average number of edges per node for a certain topology. Note that the average number of edges per node is determined by the parameters *m*, *p(add),* and *beta*. We observed that E_{mean} increases when *p(add)* and *beta* values increase. For each topology, LFAP coverage analysis is repeated for 10 topologies generated randomly by using the same BRITE parameters. E_{mean} and LFAP coverage percentage are obtained by averaging the results of these ten experiments. There are two main observations from these tables:

- As the neighborhood depth (*X*) increases the LFAP coverage percentage increases and the complete coverage is obtained using a low neighborhood depth value (i.e., X=2). This result is significant since failure notification message needs to be sent only to nodes which are two-hop away from the point of failure. This result supports that our method will provide fast convergence by introducing minimal signaling overhead within only the two-hop neighborhood.
- The topologies with higher connectivity (i.e., higher E_{mean} values) have better LFAP coverage compared to the topologies with lower connectivity (i.e., lower E_{mean} values). This is an intuitive result since the number of possible alternate hops in dense network topologies is higher than the number of possible alternate hops in sparse topologies. This phenomenon increases the likelihood of finding LFAPs, and therefore the LFAP coverage percentage.

Table 5: Coverage results for random topologies

	N	E_{mean}	LFAP Coverage Percentage (%)		
			X=0	X=1	X=2
p(add)=0.01 beta=0.01	20	3.64	82.39	98.85	100.0
	50	3.86	82.10	98.69	100.0
	100	3.98	83.21	98.03	100.0
p(add)=0.05 beta=0.05	20	3.70	85.60	99.14	100.0
	50	4.01	84.17	99.09	100.0
	100	4.08	83.35	98.01	100.0
P(add)=0.1 Beta=0.15	20	5.52	93.24	100.0	100.0
	50	6.21	91.46	99.87	100.0
	100	6.39	91.17	99.86	100.0

Table 6: Coverage results for AT&T/DFN topologies

	N	E_{mean}	Coverage Percentage (%)		
			X=0	X=1	X=2
p(add)=0.42 beta=0.62	154 (AT&T)	6.88	91.04	99.81	100.0
	30 (DFN)	8.32	93.76	100.0	100.0

CONCLUSION AND FUTURE WORK

This paper presented the testbed implementation of an innovative distributed architecture for a seamless multi-layer soft handoff in wireless battlefield networks to provide the sub-second convergence in case of link/node failures. A new alternative path calculation algorithm is proposed to calculate both local and remote LFAPs. The implementation is done in the laboratory test bed using real COTS routers and collected statistics related to the convergence times and LFAP coverage. The experiments showed that the convergence time of the remote LFAP mechanism is only slightly higher (a few 10s of milliseconds) compared to that of the local LFAP. The coverage analysis showed that, by using only a small neighborhood (e.g., 2-hop neighborhood), a complete LFAP coverage can be achieved for most topologies generated by the BRITE topology generator. The next step will include extending the alternative path calculation algorithm to cover multiple link failures. Another future work includes the LFAP selection if there are multiple LFAP candidates.

REFERENCES

[1] M. Shand and S. Bryant, “IP Fast Reroute Framework”, <draft-ietf-rtgwg-ipfrr-framework-08.txt>, February 2008 (work in progress).

[2] A. Atlas and A. Zinin, "Basic Specification for IP Fast-Rerorute: Loop-free Alternates", <draft-ietf-rtgwg-ipfrr-spec-base-012.txt>, March 2008 (work in progress).

[3] I. Hokelek, et. al., “Loop-Free IP Fast Reroute Using Local and Remote LFAPs”, <draft-hokelek-rlfap-01.txt>, February 2008 (work in progress).

[4] I. Hokelek, et. al., “Seamless Soft Handoff in Wireless Battlefield Networks using Local and Remote LFAPs”, IEEE MILCOM 2007, Orlando, FL, October 2007.

[5] Oliver Heckmann et. al., “How to use topology generators to create realistic topologies”, Technical Report, Dec 2002.